

digital signature of signature data 570 using the signatory's private key 202. The signature data 570 is data that is a function of the digital data 200. For example, the signature data could be any one of the versions of the digital data 200, a hash of any one of the versions, the universal signature object 100, or a hash of the universal signature object 100. The signature data 570 could also include any combination of the foregoing examples. Because of the functional relation between the signature data 570 and the digital data 200, any digital signature is effectively a digital signature of the digital data 200.

[0049] In an embodiment, the timestamping means 410 in the signing program 400 requests 518 a timestamp 580 from a timing source 210 for the digital signature. The timestamp is stored as part of the timestamp information 116, 126 of the USO 100. In one embodiment, the timing source 210 is a third-party timing source accessed through a network connection 308, as depicted in Figure 2. Alternatively, the signatory's computer 300, or a timing source 210 connected to the computer system 300 through a local area network connection, acts as the timing source 210. Alternatively, for greater accuracy, the timestamping means 410 obtains 518 timing information or timestamps from multiple time sources. In each of the foregoing timestamp embodiments, the timing source 210 can also digitally sign the timestamp.

[0050] With the digital signature and timestamp (if a timestamp is obtained) stored in the USO 100, the signing program 400 prompts 520 the signatory 500 to determine whether the signatory wishes to append an additional digital signature. If the signatory 500 wishes to include an additional digital signature, step 516 and optional step 518 are repeated. The additional digital signature can be of different signature data than was used in the previous digital signature. It shall be noted that the USO 100 and the hash of the USO, which each can serve as signature data, can be different than for the previous digital signature because the USO 100 includes the previous digital signature. When the signatory 500 no longer desires 520 to include an additional digital signature, the universal signature object generation is complete.

[0051] In an alternative embodiment, the signing program 400 includes a transaction tracking means 406, wherein the transaction tracking means 406 obtains, from a transaction server 220, a tracking number for audit purposes. In yet another embodiment, the transaction tracking means 406 transmits to the transaction server 220 a copy of the universal signature object 100 or a copy of a digital signature and timestamp. The transaction server 220 can store the universal signature object 100 or the digital signature for archiving, audit, and/or verification purposes.

[0052] In an embodiment, the USO generating means 408 includes 522 the signatory 500's public key 204. Including the public key 204 is beneficial because it simplifies the digital signature verification process. Verification is simplified because a person or entity trying to verify a digital signature does not need to search for the signatory's public key. Including the public key 202 in the USO 100 also makes the USO 100 a self-contained item and better suited for archiving.

[0053] In an embodiment, the USO generating means 408 includes 524 use-permission information 130. The USO generating means 408 prompts the signatory 500 to provide certain levels of use permission with respect to one or more of the versions of the digital data and/or use permission for the universal signature object 100. Using the business contract illustration, the signatory 500 may indicate that each of the versions are read-only, so that other users or recipients of the USO 100 may only view the data 200 but not edit it. Alternatively, the signatory 500 may allow for editing of some versions by certain signatories or users of the USO but not by others.

[0054] In an embodiment, the USO generating means 408 includes a universal-signature-object viewer 600. Including the USO viewer 600 in the USO 100 makes the USO 100 further self-contained because the USO viewer 600 is designed to utilize a USO 100. Thus, a third party need not search for one application to utilize a version of the digital data 200 in the USO 100, a

second application to view a digital signature, and a third application to verify the digital signature. The USO viewer is described in more detail below.

[0055] In an embodiment, the USO generating means 408 includes the signing program 400 as part of the universal signature object 100. Including the signing program 400 is beneficial because the universal signature object 100 may be transmitted or passed to additional signatories. Providing the signing program 400 with the USO 100 simplifies the process of appending signatures. In one embodiment, the process of appending a digital signature is similar to the process described for generating a USO 100. It shall be noted, however, that appending a digital signature may only require a subset of the method depicted in Figure 5. For example, steps 510, 512, and 514 may be removed from the process of appending a digital signature to an existing USO 100. It shall also be noted that the method depicted in Figure 5 is merely one embodiment.

[0056] In an embodiment, the signing program 400 compresses the USO. Alternatively, the signing program 400 encrypts the USO, for example, with a USO recipient's public key or a session key. In another embodiment, the signing program 400 interfaces with a routing service to route the USO 100 to the next recipient. The routing service may optionally return the next recipient's public key, wherein the signing program 400 encrypts the USO 100 with the recipient's public key and transmits the USO 100 via the network connection 308 directly to the recipient, transmit it via a email service, or transmit it via the routing server. Embodiments of the routing methods and systems are described in commonly-assigned U.S. Provisional Patent Application Serial No. 60/242,013, "Efficient Method For Routing Deliveries Through Recipient Translation," by Eng-Whatt Toh, filed 19 October 2000. The subject matter of the foregoing application is incorporated herein by reference in its entirety. In another embodiment, the signing program both compresses and encrypts the USO 100.

[0057] Referring now to Figure 6, an embodiment of a universal-signature-object viewer 600 is depicted. As with the signing program 400, the USO viewer 600 functions on a computer system 300 and could be represented in Figure 3 as either application 320 or 322. The USO